

Appl. No. 09/918,831  
Final Amendment and/or Response  
Reply to final Office action of 12 APRIL 2006

RECEIVED  
CENTRAL FAX CENTER

Page 7 of 10

AUG 14 2006

REMARKS / DISCUSSION OF ISSUES

Claims 1-8 and 11-16 are pending in the application.

Claim 16 stands allowed. Claims 3-5 and 12-14 were objected to, but would be allowable if rewritten in independent form including all of the limitations of their respective base claim and any intervening claims. Applicant thanks the Examiner for these indications of allowable subject matter.

Claims 1, 7 and 8 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over Rijmen et al. (hereinafter noted "Rijmen") in view of Loureiro et al. (hereinafter noted "Loureiro") and further in view of Knudsen et al. (hereinafter noted "Knudsen"); claims 2 and 11 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over Rijmen/Loureiro/Knudsen and further in view of a FOLDOC article on "brute force" (hereinafter noted "FOLDOC"); and claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over Rijmen/Loureiro/Knudsen and further in view of Isaka et al. (hereinafter noted "Isaka").

Applicant respectfully traverses these rejections.

Claims 1 and 8 are directed, respectively, to a method and a system for linear transformation in a symmetric-key cipher. The method comprises: generating a binary error-correcting code, represented by a generator matrix  $G$  in a form  $G = (I_k \parallel B)$ ; and extending matrix  $B$  with  $2k-n$  columns such that a resulting matrix  $C$  is non-singular, and deriving the linear transformation matrix  $A$  from matrix  $C$ .

As correctly conceded by the Office Action, Rijmen does not disclose, teach or suggest extending matrix  $B$  and deriving matrix  $A$  from matrix  $C$ , as recited in claims 1 and 8, and the Office Action relies upon a second reference, Loureiro, for this subject matter. However, the Office Action does not provide any suggestion or motivation in the references themselves to modify and/or combine said references. See Office Action, page 3, lines 10-14. Rather, the Office Action attempts to substitute facts within the personal knowledge of the Examiner for a motivation or suggestion to combine within the references themselves. *Id.*

Appl. No. 09/918,831  
Final Amendment and/or Response  
Reply to final Office action of 12 APRIL 2006

Page 8 of 10

Applicant respectfully submits that the Office Action's reliance on facts within the personal knowledge of the Examiner is improperly taken. According to 37 C.F.R. § 1.104(d)(2), discussed and cited in M.P.E.P. § 2144.03, the Examiner is required to submit an affidavit supporting the facts of which the Examiner relies upon, subject to contradiction or explanation by the Applicant and other persons. Applicant requests such an affidavit.

Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. See *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430, 1432 (Fed. Cir. 1990) (holding that, although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so"); see also *In re Fritch*, 972 F.2d 1260, 23 USPQ2d 1780 (Fed. Cir. 1992). Similarly, even if the references relied upon establish that all aspects of the claimed invention were individually known in the art at the time the claimed invention was made, a statement by the Examiner that modifications of the prior art to meet the claimed invention would have been within the ordinary skill of the art is not sufficient to establish a prima facie case of obviousness without some objective reason to combine the teachings of the references. See *Ex parte Levengood*, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993).

Claims 1 and 8 also recite the step of, or means for, shortening the error-correcting code. As is correctly conceded by the Office Action, the combined Rijmen and Loureiro do not disclose, teach or suggest that subject matter either. Thus, the Office Action relies upon yet another, third reference, Knudsen, for that particular subject matter.

Applicant respectfully submits that there is no suggestion or motivation, either in the three applied references themselves or in the knowledge generally available to one of ordinary skill in the art at the time the application was filed, to modify or to combine these three references by picking, choosing and combining various parts of these three references, to the exclusion of other parts of the references. Doing so requires a significantly precise motivation that is not found in any of the cited references. Rather

**Appl. No. 09/918,831**  
**Final Amendment and/or Response**  
**Reply to final Office action of 12 APRIL 2006**

**Page 9 of 10**

the only motivation to arrive at the claimed combination by picking and choosing the various parts of the applied references to the exclusion of the other parts of those references is found in the Applicant's disclosure itself.

It is therefore submitted that claim 1, and consequently also claim 8, which is directed to a system comprising means adapted to perform the method recited in claim 1, are not obvious over the cited art references.

It is submitted that claims 2, 6 and 7 are also allowable because they ultimately depend from claim 1, which is allowable over the cited art references based upon the above arguments. Accordingly, reconsideration and withdrawal of their rejections is respectfully requested.

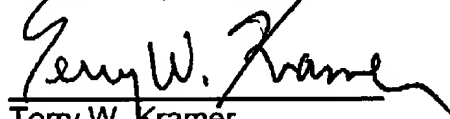
It is also submitted that claims 11 and 15 are also allowable because they ultimately depend from claim 8, which is allowable over the cited art references based upon the above arguments. Accordingly, reconsideration and withdrawal of their rejections is respectfully requested.

**Appl. No. 09/918,831**  
**Final Amendment and/or Response**  
**Reply to final Office action of 12 APRIL 2006**

**Page 11 of 11**

In view of the foregoing, applicant(s) respectfully request(s) that the Examiner withdraw the objection(s) and/or rejection(s) of record, allow all the pending claims, and find the application to be in condition for allowance. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the correspondence attorney listed below at the telephone number listed below.

Respectfully submitted,



Terry W. Kramer  
Reg. 41,541  
Attorney for Applicant

KRAMER & AMADO, P.C.  
1725 Duke Street  
Alexandria, VA 22314  
Phone: 703-519-9801  
Fax: 703-519-9802

**MAIL ALL CORRESPONDENCE TO:**  
**Eric M. Bram, Registration No. 37,285**  
**US PHILIPS CORPORATION**  
**P.O. Box 3001**  
**Briarcliff Manor, NY 10510-8001**  
**Phone: (914) 333-9635**  
**Fax: (914) 332-0615**